Maryland Acceptable Use Policy

Last Update: 01/31/2017

Contents

1.0 Purpose

Effective security is a team effort involving the participation and support of every information system user who deals with information and Information Technology (IT) assets. Defining acceptable use sets boundaries and guidance on how these IT resources are to be used. Appropriate use of Information Technology (IT) resources and effective security are integral to protecting the confidentiality, integrity, and availability of IT systems and assets. The Maryland Department of Information Technology (DoIT) requires all users of IT systems and assets to sign the attached Acceptable Use form (Appendix A), and all users with administrative privilege to sign the attached Privileged User Form (Appendix B).

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013) Section 11: Electronic Communications Policy, and associated subsections outlining Acceptable/Proper Use (11.0) and Unacceptable/Improper Use (11.1). This policy also supersedes any related policy regarding acceptable use declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy applies to all agencies in the Executive Branch of the State of Maryland, employees of those agencies, contractors and vendors supporting those agencies, and any entities or individuals using resources belonging to those agencies. This policy also applies to all IT systems and IT devices owned, leased, and/or operated by those agencies.

DoIT will be responsible for ensuring compliance with the Acceptable Use policy as outlined in section 4.0 below for Enterprise-managed agencies. Agencies under the policy authority, but not under direct management of DoIT, must independently comply with the requirements of this policy and have each employee, contractor, and vendor sign the Acceptable Use Form(s) in Appendix A and B (when applicable) during new-employee orientation and annually thereafter.

4.0 Policy

This policy outlines conduct considered acceptable and unacceptable use of resources within the DoIT infrastructure and Maryland Executive agencies.

4.1 General Acceptable Use

All uses of Maryland state IT assets and services must comply with State policies, standards, procedures, and guidelines, as well as with any applicable Federal, State or local laws.

Acceptable use of information technology assets includes the following responsibilities:

- Use information assets or services consistent with authorized assigned duties, including:

- Sending and receiving electronic mail for job related information, reports, spreadsheets, maps, etc.
- Use electronic mailing lists and file transfers to expedite official communications within and among state agencies and other job-related entities, such as vendors
- Access online information resources to gather information and knowledge directly related to job duties

- Comply with authorized levels of access, and utilize only approved information technology assets or services
- Promptly report the theft, loss, or unauthorized disclosure of an information technology asset or of proprietary information

4.2 Unacceptable Use

Engaging in unacceptable use of Maryland state IT assets is a security violation and is strictly forbidden.

The following examples are a general, non-exhaustive, list of unacceptable uses of IT assets and services:

- Engaging in any activity that is illegal under local, State, Federal or international law while using the State's information technology assets and electronic communication systems
- Creating, downloading, viewing, storing, copying, or transmitting data related to activities that reflect adversely upon the State (such as gambling, hate speech, illegal weapons, terrorist activities, pornography, and any inappropriate and/or illegal activities) that is outside the official duties and responsibilities
- Unauthorized collecting, transmitting, or sharing of confidential information, e.g., Personally Identifiable Information (PII), HIPAA (personal health) information, Federal Tax Information (subject to IRS 1075 Compliance), and Criminal Justice Information (subject to CJIS Compliance)
  - Transmitting confidential information without encryption
- Violating the rights of any person or company protected by copyright, trade secret, patent, intellectual property, or similar laws or regulations, e.g., installing or distributing software products that are either "pirated" or not appropriately licensed for use by the State or authorized for use on the network
- Unauthorized reproduction of copyrighted material, e.g., digitizing and distributing photographs from magazines, books or other copyrighted sources, copyrighted music, or installing copyrighted software for which the State does not have an active license
- Exporting software, technical information, or technology in violation of international or regional export control laws
- Intentionally introducing malicious programs into the State's electronic communication system infrastructure such as workstations, servers, and networks
- Circumventing user authentication or security of any account, host, or network, including disclosing a user's password to others or allowing a user's account to be used by others

- Interfering with or denying access to resources to any user or system, e.g., conducting a denial of service attack
- Accessing data, servers, or accounts for any purpose other than conducting official State or job related business or duties, even if the user has authorized access
- Interfering with or disrupting network users, services, or workstations, including distributing unsolicited advertising or propagating computer viruses
- Tampering with the security of State owned workstations, network equipment, services, or files
- Posting agency information to external newsgroups, bulletin boards, or other public forums without written authority
- Transmitting or storing confidential information to or from a personal email account, on a non-State issued device, or with an unapproved third-party storage service
  - Users are not allowed to use automated forwarding from a .gov account unless an exception has been granted to the user.

4.3 Privileged Users and Accounts

Privileged users (usually IT Administrators) must abide by the following additional requirements:

- **Privileged access** is only granted to authorized, qualified, individuals with a specific need for the access to perform job duties
  - Authorization for privileged access must be obtained from a Government employee who ensures that the individual has been vetted adequately by Human Resources and the privileged user's supervisor
- Users with privileged access must have two (2) user IDs
  - One for normal day to day activity (general usage)
  - One for all administrative duties
- Administrators must only use their privileged accounts to perform administrative functions
- Administrators must not:
  - Use privileged accounts to access unauthorized information, including viewing, modifying, copying, or destroying system or user data not in support of administrative functions
  - Be able to use privileged accounts to view email or browse the Internet

4.4 Email Communication Activities

When using State resources to access or use emails systems, users must exercise good judgement when opening unsolicited messages. Questions regarding email communication should be directed to a supervisor or to DoIT personnel (such as DoIT Service Desk or IT Admins).

While using State resources an end user must not:

- Send any unsolicited messages, including "junk mail" or other advertising material (email spam), to individuals who did not specifically request such material

- Engage in any form of harassment via email, telephone (including via text), or paging, whether in the form of language, frequency, or size of messages
- Engage in the unauthorized use, or forging, of email header information
- Create or forward “chain letters”, “Ponzi”, or other “pyramid” schemes of any type

4.5 Personal Use

Personal use of State information technology assets and services is permitted, provided such use is consistent with this policy, is limited in amount and duration, and does not impede or interfere with the end user’s ability to fulfill his or her assigned duties. End users must not use State information technology assets to conduct or manage personal business affairs, e.g., webhosting, real estate business, or supporting a side business.

End users must use their best judgment regarding personal use of State information technology assets. End users must not use State information technology assets for personal use in a manner that would jeopardize the security of the State or the State’s reputation.

4.6 Individual Accountability

All users are accountable for their access-related actions and will protect their credentials by following the requirements below:

- Users will not disclose passwords or let other users use their accounts on any system or network.
- Users will exercise due care when accessing State information technology resources and protect the (State’s) information from unauthorized disclosure or compromise.
  - Users are required to lock their accounts when leaving their workstations unattended as they are accountable for any activity from their account.
- Users will ensure that they maintain the security of restricted areas and locations containing restricted State IT assets, communication systems, and services against unauthorized intrusion or access, e.g., not allowing someone to “piggyback” when entering a datacenter or work location.

5.0 Exemptions

The Department of Information Technology (DoIT) has the authority to set policy and provide guidance and oversight for the security of all IT systems in accordance with Maryland Code §3A-303 and §3A-305. There is no exemption to this policy.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Account Management Policy
- Asset Management Policy
- Mobile Device Security Policy

- Remote Access Policy

7.0 Definitions

Term	Definition
Privileged Access	An access right granted to an individual, a program, or a process giving them administrative capabilities.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for ensuring compliance with the Acceptable Use policy for all Executive Branch agencies. For Enterprise on-boarded agencies, DoIT will enforce compliance with this Acceptable Use Policy according to the requirements established in section 4.0. Agencies under the policy authority of DoIT but not managed by the Enterprise will comply by ensuring all users have signed and submitted an Acceptable Use Form upon initial access and as part of a yearly refresh-training campaign. All IT administrators will also sign and submit the Privileged User Agreement Form.

If DoIT determines that an agency is not compliant with this policy, the agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After such time, if the agency remains out of compliance the Secretary of Information Technology will be notified and remediation will be mandated.

Any attempt to circumvent the Acceptable Use policy will be treated as a security violation and subject to disciplinary action which may include written notice, suspension, termination, and possible criminal and/or civil penalties.

Appendix A: Acceptable Use Form

I certify that I have read and understand the Acceptable Use Policy. I understand and acknowledge my obligations and responsibilities as outlined within the policy and will only use those access rights that I have been authorized to use, and will not reveal any of my passwords or user account identifiers (IDs), or share access with others.

I understand and acknowledge that should I become aware of any misuse of information or information systems, I am obligated to immediately inform agency management.

I understand and acknowledge that the Agency which employs me, and DoIT as the policy setting authority, reserve the right to monitor system activity and usage, including Internet activity. My signature on this document means I have consented to this monitoring.

I understand and acknowledge that there should not be any expectation of privacy or ownership. All emails, files, and documents — including personal messages, files, and documents — created, sent, received, or stored on information systems or devices owned, leased, administered, or otherwise under the custody and control of the State of Maryland are the property of the State and may be subject to review.

Notwithstanding the above, using an information system does not constitute consent to searching or monitoring of the content of privileged communication or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communication and work product are private and confidential.

I further understand and acknowledge that violation of this policy may result in disciplinary action. Depending on the severity or frequency of the violations, this could include:

1) Written notice
2) Suspension or termination of access permissions, which could result in a job reassignment
3) Termination of employment
4) Personal liability under applicable local, state, Federal, or international laws

Acknowledged and agreed to by:

_____ _____

Signature Print Name

_____

Date

Appendix B: Privileged User Agreement Form

This agreement should only be signed by users who have Privileged User or Administrative Rights and must be signed in addition to, not in lieu of, signing Appendix A: Acceptable Use Form.

I certify that I have read and understand the Information System Acceptable Use Policy as it relates to privileged (administrative) users and will only use those access rights that I have been authorized to use, and will not reveal any of my passwords, user accounts identifiers (IDs), or share access with others.

I understand and acknowledge that should I become aware of any need to access a system to which I do not have credentials, I must follow a formal request process to receive authorized, privileged access.

I understand and acknowledge that there should not be any expectation of privacy or ownership. All files and documents — including personal files and documents — created or stored on information systems or devices owned, leased, administered, or otherwise under the custody and control of the State of Maryland are the property of the State and may be subject to review. I understand and acknowledge that privileged access rights are given to individuals with a specific need for the elevated access to perform job duties, and that I must inform the Account Manager if I no longer need privileged access to a system or information.

I understand and acknowledge that I have only been authorized to use my privileged access account only for assigned, or tangentially related, administrative duties and that I will use my general usage account for normal day-to-day activities.

I understand and acknowledge that users with privileged access rights must use their account to perform only administrative functions, and must not use privilege access to view, modify, copy, or destroy a system or data without the proper authorization.

I further understand and acknowledge that violation of this policy may result in disciplinary action. Depending on the severity or frequency of the violations, this could include:

1) Written notice
2) Suspension or termination of access permissions, which could result in a job reassignment
3) Termination of employment
4) Personal liability under applicable local, state, Federal, or international laws

Acknowledged and agreed to by:

_____ _____

Signature Print Name

_____

Date